

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF OHIO
EASTERN DIVISION**

UNITED STATES OF AMERICA,)	CASE NO. 1:20-cr-186
)	
)	
PLAINTIFF,)	JUDGE SARA LIOI
)	
vs.)	
)	MEMORANDUM OPINION
STEVEN FOSTER and RICHARD EBY,)	
)	
)	
DEFENDANTS.)	

Plaintiff United States of America (the “government”) seeks a ruling from the Court *in limine* that a set of internet records it intends to offer at trial are self-authenticating under Federal Rules of Evidence 902(11) and (13) and that self-authentication of these records does not violate the Confrontation Clause. (Doc. No. 220 (Motion).) No objections or challenges have been made to the certifications. For the reasons discussed below, the government’s motion is granted.

I. BACKGROUND

In its motion *in limine*, the government asks the Court to find that a set of internet provider records is self-authenticating such that a custodian is not required to testify to the records’ authenticity. (Doc. No. 220, at 1–2.¹) In addition to its motion, the government has also submitted two supplemental filings (Doc. No 223; Doc. No. 225.) The first submits certifications of three additional providers for self-authentication. (Doc. No. 223, at 2.) The second updates the set of

¹ All page number references herein are to the consecutive page numbers applied to each individual document by the electronic filing system.

certifications identified as Exhibits 17 through 21. (Doc. No. 225, at 2.) In total, nine different internet providers disclosed records to the government, including seven domestic providers and two foreign providers. (Doc. No. 221, at 1; Doc. No. 223, at 2.) At this stage in the proceedings, the government's motion is limited to seeking a ruling authenticating the records such that they could be admitted without testimony of a custodian, as well as a ruling that the use and admission of certificates to establish the authenticity of the records does not violate the Confrontation Clause. (Doc. No. 221, at 2–3.) Regardless of the Court's ruling on the present motion, the defendants would retain the ability to challenge the records on grounds of hearsay and relevance at trial. (*Id.*)

II. MOTION *IN LIMINE*

Although not explicitly authorized by the Federal Rules of Evidence or the Federal Rules of Criminal Procedure, the practice of ruling on motions *in limine* “has developed pursuant to the district court's inherent authority to manage the course of trials.” *Luce v. United States*, 469 U.S. 38, 41 n.4, 105 S. Ct. 460, 83 L. Ed. 2d 443 (1984). Motions *in limine* allow the court to rule on evidentiary issues prior to trial in order to avoid delay and to allow parties to focus remaining time on issues that will in fact be considered by the jury. *See United States v. Brawner*, 173 F.3d 966, 970 (6th Cir. 1999); *Jonasson v. Lutheran Child & Family Servs.*, 115 F.3d 436, 440 (7th Cir. 1997). Further, *in limine* rulings are preliminary, and the district court may change its ruling at trial for any reason it deems appropriate. *United States v. Yannott*, 42 F.3d 999, 1007 (6th Cir. 1994).

The government seeks a ruling that records from nine providers are self-authenticating pursuant to the applicable rules of evidence. Seven of the providers are located in the United States. They include: (1) CenturyLink; (2) Google; (3) X (formerly, Twitter); (4) Charter

Communications; (5) Time Warner; (6) MyLOL; and (7) AT&T. (Doc. No. 220, at 2; Doc. No. 223, at 2.) Two providers, OVH (Chateen) and Kik, are from Spain and Canada, respectively.² (Doc. No. 220, at 2.) The government has provided certifications from a custodian of record for each of the above providers. (*See id*; *see also* Doc. Nos. 223, at 2; Doc. No. 225, at 2.) Additionally, the government seeks a ruling that pre-authentication of the records listed above does not violate the Confrontation Clause. (Doc. No. 220, at 3.)

The Court will first address authentication of the records individually before proceeding to consider the Confrontation Clause.

a. Authentication

The government seeks a motion *in limine* finding a total of twenty-two exhibits, comprising internet records from nine different providers, are pre-authenticated under Rules of Evidence 902(11) and 902(13). (*See generally* Doc. No. 220.) Rule 902(11) provides that evidence is self-authenticating where an original or copy of the record is certified by a custodian, and where that certification meets the requirements of the Rule 803(6)(A)–(C). Fed. R. Evid. 902(11). The relevant portion of Rule 803, commonly referred to as the business records exception, requires the evidence to meet three conditions. Fed. R. Evid. 803(6). First, the record must be “made at or near the time by – or from information transmitted by – someone with knowledge[.]” *Id.* Second, the record must be “kept in the course of a regularly conducted activity of a business[.]” *Id.* Third, making the record must be “a regular practice of that activity[.]” *Id.* Each of these requirements

² In its motion, the government stated that Exhibit 14 is a foreign record. (Doc. No. 220, at 8.) It appears the government meant to refer to Exhibit 13, as Exhibit 13 contains the records of Kik, a Canada-based company. (*See generally* Doc. No. 220-10.) Exhibit 14 contains domestic records of the company MyLOL. (*See generally* Doc. No. 220-11.) As such, the Court will treat Exhibit 13 as a foreign record and Exhibit 14 as a domestic record.

must be met “as shown by a certification of the custodian” for Rule 902(11) to apply. Fed. R. Evid. 902(11).

Additionally, the government seeks a ruling that the records are self-authenticating under Rule 902(13). (*See* Doc. No. 220, at 7.) Rule 902(13) instructs that evidence is self-authenticating when “generated by an electronic process or system that produces an accurate result, as shown by a certification of a qualified person that complies with the certification requirements of Rule 902(11) or (12).” The Court will examine each exhibit in turn, grouping exhibits from the same provider and using the same certification forms where proper.

*i. OVH (Exhibits 1–3)*³

OVH Exhibits 1 through 3 meet the requirements of 902(11) and 902(13), and the Court finds they are self-authenticating. Exhibits 1 through 3 contain internet records disclosed by OVH. (Doc. Nos. 220-1, 220-2, 220-3). Each exhibit is accompanied by a certification which provides that the records were made at or near the time of occurrence, that the records were kept in the course of regularly conducted business, and that the “business activity made such records as a regular practice[.]” (Doc. No. 220-1, at 2; Doc. No. 220-2, at 2; Doc. No. 220-3, at 1.) Additionally, the certifications provide that the record is either an original or a duplicate of the original. (Doc. No. 220-1, at 2; Doc. No. 220-2, at 2; Doc. No. 220-3, at 1.)

That the records are foreign records, as opposed to domestically-kept records, does not change the analysis. Rule 902(11) states that it applies to “domestic records” that meet the requirements of Rule 803(A)–(C). But 18 U.S.C. § 3505 provides that “[i]n a criminal proceeding.

³ Exhibits 1 and 2 are provided both in Spanish and in English translation. The Court utilizes the English translation for the purposes of this analysis.

... a foreign record of regularly conducted activity, or a copy of such record, shall not be excluded” and that a foreign record may be properly authenticated by a foreign certification. These authentications comply with the elements listed in 18 U.S.C. § 3505, and properly authenticate the records as a result. 18 U.S.C. § 3505; *see also United States v. Anekwu*, 695 F.3d 967, 977–78 (9th Cir. 2012) (foreign records presented under Rule 902(11) are properly authenticated by a foreign certification).

The OVH certifications comply with each of the requirements listed under Rule 803(6)(A)–(C), 902(11) and 902(13). As a result, the Court finds that Exhibits 1 through 3 are self-authenticating under Rules 902(11) and (13).

ii. CenturyLink (Exhibits 4 and 5)

Government’s Exhibits 4 and 5 are self-authenticating. Exhibits 4 and 5 contain domestic internet records of the company CenturyLink. (Doc. Nos. 223-1, 223-2.) The exhibits are accompanied by a certification that meets the requirements of 803(6)(A)–(C). Accordingly, Exhibits 4 and 5 are self-authenticating under both Rule 902(11) and (13).

iii. Google (Exhibits 6–8)

Government’s Exhibits 6–8 are also self-authenticating. These exhibits contain internet activity records provided by Google. (Doc. Nos. 220-4–220-6.) Each is accompanied by a certification that meets the requirements of 803(6)(A)–(C) and states that the document is a “true duplicate” of the original records. Because these certifications meet the evidentiary and statutory requirements, Exhibits 6–8 are self-authenticating under Rules 902(11) and (13).

iv. X (Exhibit 9)

Government's Exhibit 9 is self-authenticating. Exhibit 9 contains domestic internet records of the company X, formerly Twitter. (Doc. No. 223-3.) The exhibit is accompanied by a certification that meets the requirements of 803(6)(A)–(C). Accordingly, Exhibit 9 is self-authenticating under both Rule 902(11) and (13).

v. Charter (Exhibits 10 and 26)

Government's Exhibits 10 and 26 are self-authenticating. Exhibits 10 and 26 contain internet records from the company Charter. (Doc. Nos. 220-7, 220-19.) Each is accompanied by a certification that meets the requirements of 803(6)(A)–(C). Accordingly, government's Exhibits 10 and 26 are self-authenticating under Rules 902(11) and (13).

vi. Time Warner Exhibits (11–12 and 23–24)

Government's Exhibits 11–12 and 23–24 are self-authenticating. Exhibits 11–12 and 23–24 contain internet records from the company Time Warner. (Doc. Nos. 220-8, 220-9, 220-17, 220-18.) Each is accompanied by a certification that meets the requirements of 803(6)(A)–(C). Accordingly, government's Exhibits 11, 12, 23, and 24 are self-authenticating under Rules 902(11) and (13).

vii. Kik (Exhibit 13)

Government's Exhibit 13 is self-authenticating. Exhibit 13 contains internet records from the Canadian company Kik. (Doc. No. 220, 10.) The exhibit is accompanied by a certification that meets the requirements of 803(6)(A)–(C). Additionally, as explained above, the fact that the records are foreign, and not domestic, does not change the analysis. Accordingly, Exhibit 13 is self-authenticating under both Rule 902(11) and (13).

viii. MyLOL (Exhibit 14)

Government's Exhibit 14 is self-authenticating. Exhibit 14 contains domestic internet records of the company MyLOL. (Doc. No. 220-11.) The exhibit is accompanied by a certification that meets the requirements of 803(6)(A)–(C). Exhibit 14 is self-authenticating under Rules 902(11) and (13).

ix. AT&T (Exhibits 17–21)

Government's Exhibits 17–21 are self-authenticating. Exhibits 17–21 contain the records of domestic internet provider AT&T. (Doc. No. 225-1, at 1.⁴) In its original filings, the government submitted a set of certifications that did not meet the standards for self-authentication under either Rules 902(11) or 902(13). (Doc. Nos. 220-12–220-16.) But in a supplemental filing (Doc. Nos. 225-1–225-5), additional certifications were provided. These certifications each provide that the records were made at or near the time of each act, that they were made as a regular practice, and that the records were kept in the course of regularly conducted business activity. (Doc. No. 225-1, at 1.) The certifications are each signed by a custodian of the records. (Doc. No. 225-1, at 1.) Having met each of these requirements, the government's original and supplemental certifications of Exhibits 17 through 21, together, are self-authenticating under both Rules 902(11) and (13).

⁴ Each of the certifications in Exhibits 17–21 use an identical template with identical language. In its analysis, the Court refers to Exhibit 17 for simplicity.

b. Confrontation Clause

The government also requests a ruling that self-authentication of the exhibits does not violate the Confrontation Clause. The Confrontation Clause prohibits the use of testimonial evidence against a defendant without allowing for cross-examination. *Crawford v. Washington*, 541 U.S. 36, 68, 124 S. Ct. 1354, 158 L. Ed. 2d 177 (2004). Evidence is testimonial where a reasonable person would believe that it is made for use at trial. *Melendez-Diaz v. Massachusetts*, 557 U.S. 305, 310, 129 S. Ct. 2527, 174 L. Ed. 2d 314 (2009).

The Court in *Melendez-Dias* found that an affidavit identifying a substance as cocaine was testimonial evidence, and therefore could not be admitted without allowing the defendant to cross-examine the declarant. *Id.* at 307. Specifically, the Court determined that the evidence was testimonial because it was created “for the sole purpose of providing evidence against the defendant.” *Id.* at 332–23. As part of its explanation, the Court clarified that “[a] clerk could by affidavit *authenticate* or provide a copy of an otherwise admissible record.” *Id.* Accordingly, numerous courts have since found that self-authentication of records under Rule 902 does not violate the Confrontation Clause. *United States v. Anderson*, No. 22-1237, 2023 WL 3413905, at *3 (6th Cir. May 12, 2023); *United States v. Johnson*, 688 F.3d 494, 504–05 (8th Cir. 2012); *United States v. Yeley-Davis*, 632 F.3d 673, 680–81 (10th Cir. 2011).

The internet records in this case are not testimonial. The government seeks self-authentication only for the purpose of certifying that the evidence to be introduced is a true copy of the original. (Doc. No. 220, at 2.) Such a use is appropriate and amounts to “nothing more than the custodian of records . . . attesting that the submitted documents are actually records kept in the ordinary course of business.” *Yeley-Davis*, 632 F.3d at 680 (quoting *United States v. Ellis*, 460

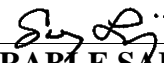
F.3d 920, 927 (7th Cir. 2006)). In this sense, self-authentication under Rule 902(11) and (13) does not violate the Confrontation Clause because it does not certify any factual assertions. *See Johnson*, 688 F.3d at 505. Because the government seeks self-authentication under Rules 902(11) and (13) only for the purpose of establishing the authenticity of the record, the Court finds that self-authentication of the exhibits does not violate the Confrontation Clause, and that the exhibits do not require testimony of a custodian for admission at trial.

III. CONCLUSION

For the foregoing reasons, the government's motion *in limine* is GRANTED. The certifications identified as Exhibits 1 through 27 are self-authenticating under Rules 902(11) and (13), and self-authentication of the documents pursuant to the Rules of Evidence does not violate the Confrontation Clause.

IT IS SO ORDERED.

Dated: January 17, 2024



HONORABLE SARA LIOI
CHIEF JUDGE
UNITED STATES DISTRICT COURT